ELSEVIER Linear Algebra and its Applications 322 (2001) 193–206

LINEAR ALGEBRA AND ITS APPLICATIONS

www.elsevier.com/locate/laa

Linear cellular automata with boundary conditions

William Chin*,[1], Barbara Cortzen[1], Jerry Goldman [2]

Department of Mathematical Sciences, DePaul University, Chicago, IL 60614, USA

Received 21 January 2000; accepted 24 July 2000

Submitted by R. Guralnick

Abstract

The main results of the paper concern graphs of linear cellular automata with boundary conditions. We show that the connected components of such graphs are direct sums of trees and cycles, and we provide a complete characterization of the trees, as well as enumerate the cycles of various lengths. Our work generalizes and clarifies results obtained previously in special cases.

Keywords: Linear cellular automata; Boundary conditions; State transition diagram

1. Introduction

A linear (or additive) cellular automaton is a system consisting of sites on a lattice, which correspond to cell processor memory having finite field elements as values, and which evolve synchronously over discrete time according to a given local interaction rule called the state transition function [11,12]. As in [7,12], we consider such automata where at most a finite number of the sites of the systems studied contain non-zero values at any instant of time and the set of such sites and site values, a configuration of sites and site values of the lattice at time t, is called the state of the system at time t. The interaction rule is a function which assigns a site value

* Corresponding author.

E-mail addresses: wchin@condor.depaul.edu (W. Chin), bcortzen@condor.depaul.edu (B. Cortzen), jgoldman@condor.depaul.edu (J. Goldman).

[1] Supported by a URC grant at DePaul University.

[2] Supported by DePaul College of Liberal Arts and Sciences research grant.

0024-3795/01/$ - see front matter
PII: S 0 0 2 4 - 3 7 9 5 (0 0) 0 0 2 2 7 - 5

at time $t+1$ to each site in terms of values at certain of its neighbors at previous time t. Several authors in the past, following the approach initiated in [7], represented states as elements of a Laurent polynomial ring and most frequently studied state transition functions which were linear. For example, see [3,5,6,7]. In this paper, we generalize the notion of a linear cellular automaton by viewing the state transition function abstractly as an endomorphism acting upon a module of states. (For a basic reference on rings and modules, see, for example, [4].) This generalizes the approach of several previous contributors and allows a conceptual understanding of the structure of cellular automata including those satisfying null and periodic boundary conditions.

Let R be a commutative Artinian ring and let M be a free R-module of finite rank. The triple $\Sigma = (R, M, \alpha)$ will be called a *generalized linear automaton* if R and M are as above and $\alpha \in \mathrm{End}_R M$. These are often referred to as "additive" cellular automata. Here, M is the set of states and α is the state transition function. In the literature, R and M have been taken as

$$R = M = \frac{F[x_1, x_2, \ldots, x_m]}{I},$$

where F is a finite field, and I is an ideal of $F[x_1, x_2, \ldots, x_m]$ which is thought of as a set of boundary conditions. When I is the ideal generated by some $x_i^{n_i}, n_i > 0$, the boundary conditions are said to be *null*, and when the generators are of the form $x_i^{n_i} - 1$, they are said to be *periodic*.

For example, if $R = M = Z_2[x]/(x^n - 1)$ and α is given by left multiplication by $\overline{x} + \overline{x}^{-1}$, then we get the "rule 90" automaton of Wolfram, extensively studied by others as well [7]. Here $\alpha(f(x)) = (x + x^{-1})f(x)$ for any $f(x) \in M$. Classically, this is rendered by giving the local transition rule $x_i(t+1) = x_{i-1}(t) + x_{i+1}(t)$, where $x_i(t)$ is the site value at position i on the one-dimensional lattice at time t.

As another example, consider the two-dimensional cellular automaton given by $R = M = Z_2[x, y]/(x^n - 1, y^m - 1)$, where α is left multiplication by $x + x^{-1} + y + y^{-1}$. Here, the cells lie on a torus and each cell value at time $t+1$ is the sum of the values of its four orthogonal neighbors at time t.

Following the seminal paper [12], the basic global approach to describing linear automata was initiated in [7] for certain periodic boundary conditions and some examples and classes of linear transition rules. The state transition graphs were associated with the automata and connected components were computed as being built out of cycles and trees, which corresponded, respectively, to "attractors" and "transients" in the time evolution of the automaton. The connected components were computed and enumerated in a range of specific examples.

More general (higher order) linear cellular automata were studied in [6]. They adapted the Laurent polynomial representation of states given by Martin et al. [7] to higher dimensions and a module theoretic setting which allowed the coefficients of these polynomials to be elements of a finite-dimensional vector space over a finite field. Their transition rules are represented as matrices with Laurent polynomial

entries. They fully characterize the transition graphs of automata without boundary conditions.

In other work, Jen [5] studied linear automata with periodic boundary conditions and invertible transition rules, utilizing the theory of linear recurrences. In [3], periodic boundary conditions were studied using the theory of circulant matrices. More recently, in [9,10] Sutner examines the regular languages associated with such automata as well as the complexity of the associated structures. More references concerning language-theoretic aspects of linear cellular automata can be found in these papers. In [8], the same author investigates linear cellular automata associated to directed graphs, obtaining periodicity and reversibility results in some cases.

In this paper, we define a generalized linear cellular automaton using an arbitrary endomorphism of the state space as described above, and associate with it its state transition graph, a directed graph whose vertices represent states (as configurations of sites and values) and whose edges represent the temporal transitions. We extend the work of earlier authors, who studied periodic boundary conditions, while complementing the boundaryless situation characterized in [6].

We assume in this paper that the boundary conditions are such that the ring R is at least artinian and, usually, finite-dimensional over a field. The state space is then a finitely generated module, usually finite, over R. Our chief goal is to describe the state transition graph of the automaton. A principal observation is that the structure of the state transition graph reduces to the theory of a single linear transformation. As a consequence of Fitting's lemma, the connected components of the graph are products of trees and cycles. Our work generalizes and clarifies results previously obtained in special cases and specific examples, which were predominately obtained via computation. Our approach reveals the essential algebraic structure in the generalized setting.

Let us outline the contents of this paper. In Section 2, we set up basic definitions and general results concerning graphs of (generalized) linear cellular automata. Here we see how the cycles and trees with fixed non-zero in-degree appear. The in-degree is seen to be the cardinality of the kernel of the transition endomorphism, a fact observed elsewhere in special cases in [3,7], and the height of a tree is its index of nilpotency. In Section 3, we deal with direct sums, and this yields a picture of the connected components of an arbitrary linear cellular automaton as cycles with rooted trees, attached to each node of the cycle. Again, this fact was observed in special cases in [3,7]. We briefly characterize balanced trees in Section 4. Finally, in Section 5, we state our results enumerating cycle lengths in terms of the order of the transition rule. We conclude with an example that was approached computationally in [7], illustrating our re sults.

2. Definitions and general results

Let R be a commutative ring, M an R-module, and let $\alpha \in \mathrm{End}_R M$. We call the triple $\Sigma = (R, M, \alpha)$ a *linear cellular automaton* (LCA) with state module M and transition rule α.

The *graph* $\Gamma(\Sigma)$ of the LCA $\Sigma = (R, M, \alpha)$ is the directed graph whose vertices are elements of M, and whose edges are the ordered pairs (m, m'), with $m' = \alpha(m)$, for all $m \in M$ (symbolized by $m \mapsto \alpha(m)$). Note that $\Gamma(\Sigma)$ is simply the functional digraph of α, and it depends only on α and M, not on R.

If $\alpha(m) = m'$, then m' is a *successor* of m, and m is a *predecessor* of m'. If $m \in M$ has no predecessors, that is, if $m \notin \alpha(M)$, then m is called a *source* (or, as some authors prefer, a "garden of Eden"). Call m a *sink* if $\alpha(m) = m$, that is, if $\Gamma(\Sigma)$ has a loop at m.

A *tree* in this paper is a rooted tree in the usual sense, except it is a directed graph with all edges oriented towards the root, and, in addition, there is a loop attached to the root. Thus, a tree has a unique sink, namely, the root. The *height* of a tree is the number of directed edges along the longest path to the root, not including the loop at the root.

We call a finite directed graph a *cycle*, if it is connected and each vertex has a unique predecessor and a unique successor.

Proposition 2.1. *Let $\Sigma = (R, M, \alpha)$ be an LCA, where M is a finite, non-zero R-module.*

(i) *If α is nilpotent with index of nilpotency k, then the graph of Σ is a tree of height k (with a loop at the root 0). Each vertex of the tree which is not a source has $|\ker(\alpha)|$ predecessors. The number of non-sources is $|M|/|\ker(\alpha)|$, and 0 is the only sink.*

(ii) *If α is an automorphism of finite order r, then the graph of (R, M, α) is a union of cycles and all cycle lengths divide r. There is always at least one cycle of length 1 (namely, 0 with a loop).*

(iii) *Conversely, if the graph of Σ is a tree, then α is nilpotent, and if it is union of cycles, then α is an automorphism.*

Proof. (i) The first assertion of (i) is self-evident. Let $m \in M$ be a non-source, that is, $m \in \alpha(M)$. If $m = \alpha(m_1)$ for some $m_1 \in M$, then $\alpha^{-1}(m) = m_1 + \ker(\alpha)$, and therefore there are $|\ker(\alpha)|$ predecessors of m.

The set of all non-sources is $\alpha(M) \simeq M/\ker(\alpha)$, and, obviously, $\alpha(m) = m$ implies that $m = 0$, which proves the last statement of (i).

(ii) Obviously, each element $m \in M$ has a unique predecessor $\alpha^{-1}(m)$, and a unique successor $\alpha(m)$. Moreover, for every $m \in M$, the size of the orbit of m, $\{\alpha^i(m)\}$ must divide r.

(iii) is self-evident. □

If $\Sigma = (R, M, \alpha)$ is an LCA with α nilpotent, we shall call the number $|\ker(\alpha)|$ the *in-degree* of the tree $\Gamma(\Sigma)$.

Example 1. Let $R = M = Z_2[x]/(x^3)$, and $\alpha =$ multiplication by $\overline{x}^2$. The graph of $\Sigma = (R, M, \alpha)$ is the tree of height 2 and in-degree 4 as shown in Fig. 1. (Here and subsequently the obvious orientation of the edges will be omitted.)

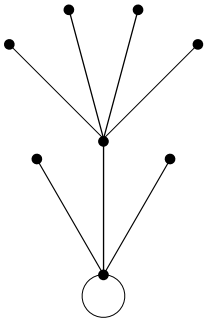


Fig. 1.

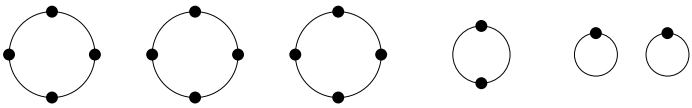


Fig. 2.

Example 2. Let $R = M = Z_2[x]/(x^4 - 1)$, and $\alpha =$ multiplication by $\overline{x}$. Then the graph of $\Sigma = (R, M, \alpha)$ is the union of three cycles of length 4, one cycle of length 2, and two cycles of length 1, as shown in Fig. 2.

3. Direct sums of graphs and LCAs

Definition 1. Let Γ_1 and Γ_2 be two directed graphs with sets of vertices M_1 and M_2, respectively. We define the *direct sum* $\Gamma_1 \oplus \Gamma_2$ to be the directed graph with the set of vertices $M_1 \times M_2$, and edges $(m_1, m_2) \mapsto (m_1', m_2')$ whenever $m_1 \mapsto m_1'$ in Γ_1 and $m_2 \mapsto m_2'$ in Γ_2. What we call here the direct sum is usually referred to as the synchronous (or direct) product in Automata Theory.

Definition 2. With above notation, directed graphs Γ_1 and Γ_2 are *isomorphic* (written $\Gamma_1 \simeq \Gamma_2$), if there is a 1–1 mapping ϕ from M_1 onto M_2, which preserves the directed edges.

Definition 3. Let $\Sigma_1 = (R_1, M_1, \alpha_1)$ and $\Sigma_2 = (R_2, M_2, \alpha_2)$ be LCAs. Then $M_1 \oplus M_2$ is an $R_1 \oplus R_2$-module, and $\alpha_1 + \alpha_2$ is in $\mathrm{End}_{R_1 \oplus R_2}(M_1 \oplus M_2)$. So $\Sigma = (R_1 \oplus R_2,\ M_1 \oplus M_2,\ \alpha_1 + \alpha_2)$ is an LCA. We call Σ the *direct sum* of the LCAs Σ_1 and Σ_2 and write $\Sigma = \Sigma_1 \oplus \Sigma_2$.

Proposition 3.1. *With above notation,* $\Gamma(\Sigma_1 \oplus \Sigma_2) \simeq \Gamma(\Sigma_1) \oplus \Gamma(\Sigma_2)$.

Proof. The vertex sets of both graphs are $M_1 \times M_2$. Furthermore, if $(m_1, m_2) \mapsto (m_1', m_2')$ in $\Gamma(\Sigma_1 \oplus \Sigma_2)$, then $(\alpha_1 + \alpha_2)(m_1, m_2) = (m_1', m_2')$ in $\Sigma_1 \oplus \Sigma_2$, that is, $\alpha_1(m_1) = m_1'$ and $\alpha_2(m_2) = m_2'$. Consequently, $(m_1, m_2) \mapsto (m_1', m_2')$ in $\Gamma(\Sigma_1) \oplus \Gamma(\Sigma_2)$. □

Proposition 3.2. *Suppose M is an R-module, $M = M_1 \oplus M_2$ (an inner direct sum of R-submodules), and α an endomorphism of M with $\alpha(M_1) \subset M_1$ and $\alpha(M_2) \subset M_2$. Then $\Gamma(R, M, \alpha) \simeq \Gamma(R, M_1, \alpha|_{M_1}) \oplus \Gamma(R, M_2, \alpha|_{M_2})$.*

Proof. The same as above with $R_1 = R_2 = R$, $\alpha_1 = \alpha|_{M_1}$, and $\alpha_2 = \alpha|_{M_2}$. (Whether we consider $M = M_1 \oplus M_2$ an R-module or an $R \oplus R$-module does not have any effect on the graph.) □

Theorem 3.3. *Let Γ_1 and Γ_2 be connected components of graphs of LCAs.*

(i) *Suppose Γ_1 is a cycle of length m and Γ_2 a cycle of length n. Then $\Gamma_1 \oplus \Gamma_2$ is a union of cycles of length* $\mathrm{lcm}(m, n)$.

(ii) *Suppose Γ_1 and Γ_2 are graphs of LCAs which are trees. Then $\Gamma_1 \oplus \Gamma_2$ is a tree whose height is the maximum of the heights of Γ_1 and Γ_2. The in-degree of Γ is the product of the in-degrees of the component trees.*

(iii) *Suppose Γ_1 is an m-cycle and Γ_2 is a graph of an LCA which is a tree. Then $\Gamma = \Gamma_1 \oplus \Gamma_2$ is an m-cycle with an isomorphic copy of the tree attached to each of its nodes, which replace the root of the tree.*

Proof. (i) Given a cycle of length m, $c_1 \mapsto c_2 \mapsto \cdots \mapsto c_m \mapsto c_1$, its orbit determines the permutation $\gamma = (c_1, c_2, \ldots, c_m)$, with $\mathrm{o}(\gamma) = m$. (If α is the underlying endomorphism of the LCA, then γ is the restriction of α to the orbit of the cycle.) Suppose Γ_1 and Γ_2 are graphs which are cycles of lengths m and n, respectively, and γ_1, γ_2 their associated permutations. Then $\mathrm{o}(\gamma_1) = m$ and $\mathrm{o}(\gamma_2) = n$. If (c_1, c_2) is a vertex of $\Gamma_1 \oplus \Gamma_2$, then the connected component of $\Gamma_1 \oplus \Gamma_2$ containing (c_1, c_2) is $(c_1, c_2) \mapsto (\gamma_1(c_1), \gamma_2(c_2)) \mapsto \cdots \mapsto (\gamma_1^l(c_1), \gamma_2^l(c_2)) = (c_1, c_2)$, where $l = \mathrm{lcm}(m, n)$. In other words, (c_1, c_2) is a vertex of a cycle whose associated permutation acts as a product of disjoint permutations (cycles) of orders m and n, respectively.

(ii) Suppose Γ_1 and Γ_2 are trees with in-degrees n_1 and n_2, and roots r_1 and r_2, respectively. Let m_1 be a vertex in Γ_1 and m_2 a vertex in Γ_2. If either m_1 or m_2 is a source, then (m_1, m_2) is a source in $\Gamma_1 \oplus \Gamma_2$. If m_1 and m_2 are not sources, and p_1 and p_2 are their respective predecessors, then $(p_1, p_2) \to (m_1, m_2)$ is a directed edge in $\Gamma_1 \oplus \Gamma_2$. Since there are n_1 choices for p_1 and n_2 choices for p_2, we conclude that every non-source in $\Gamma_1 \oplus \Gamma_2$ has n_1 and n_2 predecessors. The root of $\Gamma_1 \oplus \Gamma_2$ is (r_1, r_2), which is also the only vertex with a loop. Since every vertex in Γ_i has a unique successor for $i = 1, 2$, the same is true of $\Gamma_1 \oplus \Gamma_2$, and all its edges are directed toward the root. Moreover, suppose the height of Γ_1 is h and the height

of $\Gamma_2 \leqslant h$. If $v_1 \to v_2 \to \cdots \to v_h = r_1$ is a path of maximum length in Γ_1 (not using the loop at r_1), then $(v_1, r_2) \to (v_2, r_2) \to \cdots \to (v_h, r_2) = (r_1, r_2)$ provides a path with length h in $\Gamma_1 \oplus \Gamma_2$, and, clearly, no longer path exists in $\Gamma_1 \oplus \Gamma_2$ if one does not use the loop at (r_1, r_2).

(iii) Suppose Γ_1 is the cycle $c_1 \mapsto c_2 \mapsto \cdots \mapsto c_m \mapsto c_1$ with the associated permutation $\gamma = (c_1, c_2, \ldots, c_m)$ and Γ_2 is a tree rooted at r with in-degree n. Then $(c_1, r) \mapsto (c_2, r) \mapsto \cdots \mapsto (c_m, r) \mapsto (c_1, r)$ is the isomorphic copy of the cycle Γ_1 in $\Gamma_1 \oplus \Gamma_2$. Now each (c_i, r) has n predecessors, namely, the vertices $(\gamma^{-1}(c_i), t)$, where t's are predecessors of r. If t is a vertex of the tree Γ_2 at the level l, then $(\gamma^{-l}(c_i), t)$ is the corresponding vertex of the tree in $\Gamma_1 \oplus \Gamma_2$ which has the root (c_i, r). If t is a source in Γ_1, then $(\gamma^{-l}(c_i), t)$ is a source in $\Gamma_1 \oplus \Gamma_2$. Otherwise, t has n predecessors in Γ_2, and $(\gamma^{-l}(c_i), t)$ has the same number of predecessors in $\Gamma_1 \oplus \Gamma_2$, namely, the set $\{(\gamma^{-l-1}(c_i), s) \mid s$ is a predecessor of t in $\Gamma_2\}$. Thus, the tree with the root (c_i, r) in $\Gamma_1 \oplus \Gamma_2$ is an isomorphic image of the tree Γ_1. However, the loop at the root of Γ_2 is missing in $\Gamma_1 \oplus \Gamma_2$, or rather, it is replaced by a copy of the cycle Γ_1. □

The example below illustrates how a graph of an indecomposable R-module decomposes into a direct sum of two graphs, and how changing R to the ring $k[\alpha]$ yields a corresponding decomposition of the module M.

Example 3. The tree in Example 1 (Fig. 1) is the direct sum of trees which are graphed in Fig. 3. In Example 1, $R = M = Z_2[x]/(x^3)$, $\alpha = \overline{x}^2$, and M is an indecomposable R-module. However, if we form $R' = Z_2[\alpha] = \{0, 1, \overline{x}^2, 1 + \overline{x}^2\}$, then the graph of $\Sigma' = (R', M, \alpha)$ is identical to the graph of $\Sigma = (R, M, \alpha)$, since it depends only on the action of α on the module, the base ring being irrelevant. Now as R'-modules, $M = M_1 \oplus M_2$, where $M_1 = R'$ and $M_2 = \{0, \overline{x}\}$. That is, M can be decomposed into a direct sum of α-invariant Z_2-subspaces. $\Gamma(\Sigma')$ is thus the direct sum of the graphs of $(R', M_1, \alpha|_{M_1})$ and $(R', M_2, \alpha|_{M_2})$ as shown in Fig. 3.

Example 4. Let $\Sigma_1 = (R, M, \alpha)$, where $R = M = Z_2[x]/(x^4)$ and α is multiplication by $\overline{x}^2$. Then the graph Γ_1 of Σ_1 is the tree of height 2 and in-degree 4, in which each branch has the same height. Let Γ_2 be any 4-cycle. Then $\Gamma_1 \oplus \Gamma_2$ is the graph shown in Fig. 4.

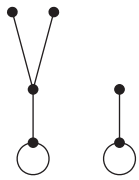


Fig. 3.

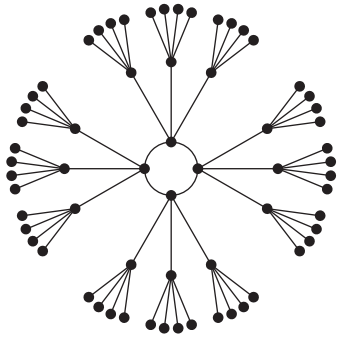


Fig. 4.

Theorem 3.4. *Let $\Sigma = (R, M, \alpha)$, where M is a finite R-module, and R a finite ring. Then the $\Gamma(\Sigma)$ is a union of direct sums of cycles and identical copies of a tree.*

Proof. As a consequence of Fitting's lemma, M can be decomposed into a direct sum of submodules M_1 and M_2, such that $\alpha|_{M_1}$ is nilpotent, and $\alpha|_{M_2}$ is an automorphism. The graph of $(R, M_1, \alpha|_{M_1})$ is a tree, while the graph of $(R, M_2, \alpha|_{M_2})$ is a union of cycles. Thus, $\Gamma(\Sigma)$ consists of all the cycles from the latter, with the tree of the former graph attached to each node of the cycle by the root. □

4. Balanced trees

In this section, we discuss LCAs $\Sigma = (R, M, \alpha)$, where R is a finite K-algebra, M a finite R-module and α a nilpotent R-endomorphism of M with $\alpha^k = 0$, $\alpha^{k-1} \neq 0$. As noted in Section 2, the graph of Σ is a tree, and if $\dim_K \ker(\alpha) = s$, then $|K|^s$ is the in-degree of the tree, that is, the number of predecessors of each non-source.

Informally, we say that a tree is balanced, if the height of every branch is the same, that is, if any path leading from any source to 0 is of equal length, say k. This is equivalent to saying that any source $a \notin \alpha(M)$ has the property that $\alpha^{k-1}(a) \neq 0$. In other words, a tree is balanced if $\ker(\alpha^{k-1}) \subset \alpha(M)$. Since the reverse inclusion always holds, we can now adopt the following formal definition, which concurs with [1].

Definition 4. If $\Sigma = (R, M, \alpha)$ is as above (with α nilpotent of index k), then we call the graph of Σ a *balanced* tree if $\alpha(M) = \ker(\alpha^{k-1})$.

Theorem 4.1. *Let $\Sigma = (R, M, \alpha)$ be as above and denote $n = \dim_K M$. Then the following are equivalent*:

(i) *The graph of Σ is a balanced tree, that is, $\alpha(M) = \ker(\alpha^{k-1})$.*

(ii) $\ker(\alpha) = \alpha^{k-1}(M)$.

(iii) $\alpha^{k-i}(M) = \ker(\alpha^i)$ *for all* $i = 1, \ldots, k$ (*with* $\alpha^0(M)$ *denoting* M).

Proof. Consider the following chain of submodules of M and view them as K-subspaces of M:

$$0 \subset \alpha^{k-1}(M) \subset \alpha^{k-2}(M) \subset \cdots \subset \alpha(M) \subset M$$

and

$$0 \subset \ker(\alpha) \subset \ker\left(\alpha^2\right) \subset \cdots \subset \ker\left(\alpha^{k-1}\right) \subset M.$$

Obviously we have $\alpha^{k-i}(M) \subset \ker(\alpha^i)$ for all i. Moreover, as vector spaces, $M \simeq \alpha^i(M) \oplus \ker(\alpha^i)$, in particular, $M \simeq \alpha(M) \oplus \ker(\alpha)$, and $M \simeq \alpha^{k-1}(M) \oplus \ker(\alpha^{k-1})$.

(i) $\Rightarrow$ (ii): Suppose the tree is balanced, that is, $\alpha(M) = \ker(\alpha^{k-1})$. Then the last isomorphism above gives

$$\begin{aligned}\dim_K\left(\alpha^{k-1}(M)\right) &= n - \dim_K \ker\left(\alpha^{k-1}\right)\\ &= n - \dim_K \alpha(M)\\ &= n - (n-s)\\ &= s,\end{aligned}$$

which implies that $\alpha^{k-1}(M) = \ker \alpha$.

(ii) $\Rightarrow$ (iii): If $\ker(\alpha) = \alpha^{k-1}(M)$, then $\ker(\alpha) \subset \alpha^i(M)$ for all $i = 1, \ldots, k-1$, and the sequence

$$0 \to \ker(\alpha) \to \alpha^i(M) \xrightarrow{\alpha} \alpha^{i+1}(M) \to 0$$

is exact for $i = 0, 1, \ldots, k-2$. Hence, we have the isomorphism of vector spaces $\alpha^i(M) \simeq \ker(\alpha) \oplus \alpha^{i+1}(M)$, which implies that $\alpha^i(M) \simeq (\ker(\alpha))^{k-i}$ (that is, $\alpha^i(M)$ is isomorphic to the direct sum of $k-i$ copies of the vector space $\ker(\alpha)$) for $i = 0, \ldots, k-1$. Thus, $\dim_K \alpha^i(M) = (k-i)s$, in particular, $\dim_K M = n = ks$, and $\dim_K \ker(\alpha^i) = n - (k-i)s = n - ks + is = is$. But $\alpha^{k-i}(M) \subset \ker(\alpha^i)$. Since the dimensions of both are i's, they must be equal.

(iii) $\Rightarrow$ (i): Obvious. □

Corollary 4.2. *With notation as in Theorem* 4.1, *the graph of Σ is a balanced tree if an only if $n = ks$, that is, if $\dim_K M = k \cdot \dim_K \ker(\alpha)$.*

Proof. If the graph of Σ is a balanced tree, then the proof of Theorem 4.1 implies that $n = ks$. On the other hand, an imbalanced tree would have fewer vertices than a balanced one (assuming the same k and s). Therefore, if a tree has the maximum number of elements, namely, $|K|^{ks}$, it must be balanced. □

Corollary 4.3. *Let T_1 and T_2 be two balanced trees which are graphs of LCAs over the same field K. Then $T_1 \oplus T_2$ is balanced if and only if T_1 and T_2 have equal height.*

Proof. Follows from a dimension count. □

5. Enumeration of cycles

In this section, we assume that R is a finite K-algebra, where K is a finite field, and M is a finite R-module.

We begin by describing a series of reductions that greatly simplifies the problem of a graph of an arbitrary LCA, using a direct sum decomposition of the graph. We remark that the graph of (R, M, α) depends only on the action of α on M, not on the structure of R. We can form a subring $K[\alpha]$ of $\mathrm{End}_R M$ and view M as a $K[\alpha]$-module via the natural extension of $\alpha \cdot m = \alpha(m)$. It is easy to see that the graphs of (R, M, α) and $(K[\alpha], M, \alpha)$ will be identical.

By the Krull–Schmidt–Azumaya theorem, the $K[\alpha]$-module M is a unique (up to isomorphism) finite direct sum of indecomposable modules. But any such indecomposable module is either $K[\alpha]$ itself, or a homomorphic image of $K[\alpha]$, since $K[\alpha]$ is the image of the principal ideal domain $K[x]$ (see, for example, [4]). So the graph of $(K[\alpha], M, \alpha)$ is uniquely the direct sum of graphs of LCAs of the form $(K[\alpha], K[\alpha], \alpha)$ and $(K[\alpha], K[\alpha'], \alpha')$, where α' is the image of α under a homomorphism from $K[\alpha]$. However, as we have already observed before, the graph of the latter is isomorphic to the graph of $(K[\alpha'], K[\alpha'], \alpha')$. In other words, our study of graphs reduces to the case of LCAs of the form $(K[\alpha], K[\alpha], \alpha)$.

Furthermore, by Fitting's lemma, we can assume that α is either a unit or that α is nilpotent. In the former case, $K[\alpha] \simeq K[x]/(f(x))$, where $f(x)$ is a factor of $x^n - 1$ (n being the order of α), and by [2], $f(x)$ is a power of an irreducible polynomial in $K[x]$. In the latter case, $K[\alpha] \simeq K[x]/(x^k)$. In either case, $K[\alpha]$ is a local ring.

In view of our results on direct sums of graphs of LCAs, we may therefore restrict ourselves to graphs of LCAs of the form (R, M, α), where $R = M = K[\alpha]$ is a local ring.

We now specialize to a field K of p elements, for a prime p. In what follows, we describe the graph of an LCA $\Sigma = (R, M, \alpha)$, where R is a finite K-algebra, α an R-automorphism of M, assuming that R is a local ring and $R = M = K[\alpha]$.

The following three theorems address the cases where the order of α is p-free, a power of p, and finally, the mixed case where $\mathrm{o}(\alpha) = sp^b$, where $b \geqslant 1$ and $p \nmid s$.

Theorem 5.1. *Suppose* $\mathrm{o}(\alpha) = s$, *where* $p \nmid s$, *and f is the order of p modulo s, that is, the least positive integer d such that* $p^d \equiv 1 (\mathrm{mod}\ s)$. *Then the graph of* Σ *consists of one cycle of length* 1, *and* $(p^f - 1)/s$ *cycles of length s.*

Proof. If p does not divide $\mathrm{o}(\alpha) = s$, then by [2, p. 95], the minimal polynomial of α is an irreducible polynomial $F(x) \in K[x]$ of degree $f =$ order of p modulo s. Thus, $K[\alpha] \simeq K[x]/(F(x))$ is a field extension on K of degree f. Therefore, every non-zero element a of $K[\alpha]$ is a unit and lies on a cycle of length s, namely, on $(a, \alpha(a), \alpha^2(a), \ldots, \alpha^{s-1}(a))$. It follows that there is one 0-cycle of length 1, and $(p^f - 1)/s$ cycles of length s. □

Theorem 5.2. *Suppose* $o(\alpha) = p^b$ *for some positive integer b. The minimal polynomial of* α *in* $K[x]$ *is then* $(x-1)^e$ *for some e with* $p^{b-1} < e \leqslant p^b$. *The graph of* Σ *consists of p cycles of length* 1, $(p^{p^a} - p^{p^{a-1}})/p^a$ *cycles of length* p^a *for* $0 < a < b$, *and* $(p^e - p^{p^{b-1}})/p^b$ *cycles of maximal length* p^b.

Proof. Since α satisfies the polynomial $x^{p^b} - 1 = (x-1)^{p^b}$, the minimal polynomial of α is of the form $(x-1)^e$, where e is some integer with $p^{b-1} < e \leqslant p^b$. Thus, $K[\alpha] \simeq K[x]/(x-1)^e$ with $\alpha \to \overline{x}$. Let $U_l = \operatorname{ann}_R(\overline{x}^l - 1)$ for $l \mid m$, that is, for $l = p^a$, where $a \leqslant b$. Then U_l is a subspace of R consisting of elements that are on cycles of length $\leqslant l$, that is, on cycles whose length divides l.

If $l = p^a$, where $p^a \leqslant e$, then $U_l = (\overline{x}-1)^{e-l} = (\overline{x}-1)^{e-p^a}$, which is the subspace of R of dimension $l = p^a$. (As a vector space, $U_l = K[(\overline{x}-1)^{e-p^a}] + K[(\overline{x}-1)^{e-p^a+1}] + \cdots + K[(\overline{x}-1)^{e-1}]$.) Otherwise, if $l = p^b$, then $\operatorname{ann}_R(\overline{x}^l - 1) = R$.

Consequently, if $e = p^b$, then $\dim_K(U_l) = l$ for all $l \mid p^b$, and if $e < p^b$, then $\dim_K(U_l) = \min(l, e)$. Thus, we have a filtration of subspaces U_l for $l = 1, p, \ldots, p^{b-1}, p^b$ with dimensions $1, p, \ldots, p^{b-1}, p^e$. This shows that the graph of Σ consists of p cycles of length 1, $(p^{p^a} - p^{p^{a-1}})/p^a$ cycles of length p^a for $0 < a < b$, and $(p^e - p^{p^{b-1}})/p^b$ cycles of maximal length p^b. □

Example 5. Let $p = 2$, $R = K[x]/(x-1)^5$, $\alpha =$ multiplication by $\overline{x}$. Then $o(\alpha) = 8$ and the graph of Σ consists of two cycles of length 1, one cycle of length 2, three cycles of length 4, and two cycles of length 8.

Theorem 5.3. *Let* $o(\alpha) = m = p^b s$, *where p does not divide s, and* $b \geqslant 1$. *Then the minimal polynomial of* α *over K is of the form* $F(x)^e$, *where* $F(x)$ *is an irreducible polynomial over K of degree* $f =$ *the order of p modulo s, and e is a positive integer. The graph of* Σ *is a union of cycles of lengths* sp^a *for all* $1 \leqslant a \leqslant b$, *and a single cycle of length* 1. *Let* $q = p^f$. *The number of cycles of length* sp^a *is*

$$\frac{q^{p^a} - q^{p^{a-1}}}{sp^a}$$

for $1 \leqslant a < b$, *and the number of cycles of length* sp^b *is*

$$\frac{q^e - q^{p^{b-1}}}{sp^b}.$$

Proof. Since $o(\alpha^{p^b}) = s$ and p does not divide s, the minimal polynomial of α^{p^b} over K is an irreducible polynomial $F(x) \in K[x]$ of degree $f =$ the order of p modulo s. Thus, we have $F(\alpha^{p^b}) = [F(\alpha)]^{p^b} = 0$, and the minimal polynomial of α over K must be $F(x)^e$ for some number e with $p^{b-1} < e \leqslant p^b$, which shows that $R = K[\alpha] \simeq K[x]/(F(x)^e)$.

As before, let $U_l = \operatorname{ann}_R(x^l - 1)$ for $l \mid m$, that is, U_l is the subspace of elements that are on cycles of length dividing l. We first observe that $U_l = 0$ unless $l = p^a s$, where a is a non-negative integer $\leqslant b$. Obviously, the only divisors of m are of the form $l = rp^a$, where $r \mid s$. Moreover, if $\operatorname{ann}(x^l - 1) \neq 0$, then $F(x) \mid (x^l - 1) = (x^r - 1)^{p^a}$, and consequently $F(x) \mid (x^r - 1)$. However, if $r \mid s$ and $r \neq s$, then none of the rth roots of 1 are primitive sth roots of 1 over K. Since, by [2], $F(x)$ is the product of factors of the form $x - \omega$, where ω's are (certain) primitive sth roots of 1, we conclude that $F(x)$ does not divide $x^r - 1$, and therefore there are no cycles in Σ of length rp^a for $r \mid s,\ r \neq s$. In other words, the only possible cycle lengths are sp^a and 1.

We now proceed to compute the number of cycles of length $l = sp^a$, with $1 \leqslant a \leqslant b$. We observe that

$$U_l = \operatorname{ann}_R\big(x^l - 1\big) = \operatorname{ann}_R\big(x^s - 1\big)^{p^a} = \big(F^{e-p^a}\big).$$

So we have a chain of subspaces

$$U_1 \subset U_{p^0 s} \subset U_{p^1 s} \subset U_{p^2 s} \subset \cdots \subset U_{p^{(b-1)} s} \subset U_{p^b s}$$

with dimensions, respectively, $q^0 = 1,\ q^{p^0} = q, q^{p^1}, \ldots, q^{p^{b-1}}, q^e$ (where $q = p^f$). That is, there is a single cycle of length 1,

$$\frac{q^{p^a} - q^{p^{a-1}}}{sp^a}$$

cycles of length $p^a s$ if $1 \leqslant a < b$, and

$$\frac{q^e - q^{p^{b-1}}}{sp^b}$$

cycles of maximal length p^b. □

Example 6. Let $K = Z_2,\ R = M = K[x]/(x^{12} - 1)$, and let α be the endomorphism of M given by multiplication by $\overline{x} + \overline{x}^{-1}$, that is, $\alpha = \overline{x} + \overline{x}^{11}$. This is the type of LCA studied extensively in [7], where the graph of this particular case is given (not quite correctly) on p. 221. The graph of $\Sigma = (R, M, \alpha)$ is provided in Fig. 7. We show here how M can be decomposed into $K[\alpha]$-modules, and how one can obtain the graph of Σ by generating the graphs of the indecomposable direct summands of the $K[\alpha]$-module M.

We immediately get the decomposition

$$M = K[x]\big/\big(x^{12} - 1\big) \simeq K[x]/\big(x + 1\big)^4 \oplus K[x]\big/\big(x^2 + x + 1\big)^4.$$

If we set $M_1 = K[x]/(x + 1)^4$ and $M_2 = K[x]/(x^2 + x + 1)^4$, then $\alpha|_{M_1}$ is nilpotent, and $\alpha|_{M_2}$ is an automorphism.

Let us now consider the LCA $(K[\alpha_1], M_1, \alpha_1)$, where $\alpha_1 = \alpha|_{M_1}$. Then $\alpha_1 = \overline{x} + \overline{x}^3$, and $\alpha_1^2 = 0$. Now $M_1 = K[\alpha_1] \oplus \overline{x}K[\alpha_1]$ as a $K[\alpha_1]$-module. The graphs

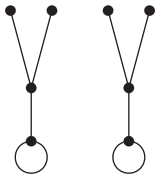


Fig. 5.

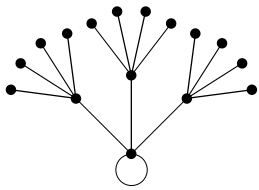
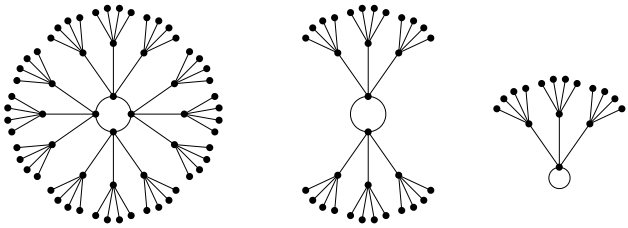


Fig. 6.



60 copies 6 copies 4 copies

Fig. 7.

of the LCAs $(K[\alpha_1], K[\alpha_1], \alpha_1)$ and $(K[\alpha_1], \overline{x}K[\alpha_1], \alpha_1)$ are trees of height 2 and in-degree 2, as shown in Fig. 5.

The graph of $(K[\alpha_1], M_1, \alpha_1)$ is their direct sum, that is, a tree of height 2 and in-degree 4 (Fig. 6).

We now proceed to examine the LCA $(K[\alpha_2], M_2, \alpha_2)$, where $\alpha_2 = \alpha|_{M_2}$. In M_2 we have the relation $\overline{x}^8 = \overline{x}^4 + 1$, so that $\alpha_2 = \overline{x} + \overline{x}^3 + \overline{x}^7$, $\alpha_2^2 = \overline{x}^6$, $\alpha_2^3 = \overline{x}^5 + \overline{x}^7$, and $\alpha_2^4 = 1$. As a $K[\alpha_2]$-module, $M_2 = K[\alpha_2] \oplus \overline{x}K[\alpha_2]$. Thus, by the Theorem 5.2, the graph of $(K[\alpha_2], K[\alpha_2], \alpha_2)$ consists of two cycles of length 1, one cycle of length 2, and three cycles of length 4. Since $\overline{x}K[\alpha_2] \simeq K[\alpha_2]$ as $K[\alpha_2]$-modules, the graph of $(K[\alpha_2], \overline{x}K[\alpha_2], \alpha_2)$ is an isomorphic copy of the former graph, thus consisting of two cycles of length 1, one cycle of length 2 and three cycles of length 4.

Taking the direct sum of these two isomorphic graphs, we obtain the graph of $(K[\alpha_2], M_2, \alpha_2)$. It consists of four cycles of length 1, six cycles of length 2 (two direct sums of the 1-cycles and the 2-cycle, two direct sums of the 2-cycle and the 1-cycles, and two 2-cycles which arise from the direct sum of the 2-cycle and the 2-cycle), and $6 + 6 + 6 \cdot 2 + 9 \cdot 4 = 60$ cycles of length 4.

Finally, the graph of the original LCA $(K[\alpha], M, \alpha)$ consists of the 70 cycles enumerated above, with a copy of the tree in Fig. 6 attached to each node (see Fig. 7).

References

[1] R. Barua, Additive cellular automata and matrices over finite fields, Indian Statistical Institute Technical Report No. 17/91, 1991.
[2] C. Curtis, I. Reiner, Methods of Representation Theory, vol. I, Wiley, New York, 1981.
[3] Pu-hua Guan, Yu He, Exact results for deterministic cellular automata with additive rules, J. Statist. Phys. 43 (3/4) (1986).
[4] T. Hungerford, Algebra. Holt, Rinehart & Winston, New York, 1974.
[5] E. Jen, Linear cellular automata and recurring sequences in finite fields, Comm. Math. Phys. 119 (1998) 13–28 (1988).
[6] L. LeBruyn, M. Van de Bergh, Algebraic properties of linear cellular automata, Linear Algebra Appl. 157 (1991) 217–234.
[7] O. Martin, A. Odlyzko, S. Wolfram, Algebraic properties of cellular automata, Comm. Math. Phys. 93 (1984) 219–258.
[8] K. Sutner, Sigma-automata and Chebyshev polynomials, Theoret. Comput. Sci. 230 (1–2) (2000) 49–73.
[9] K. Sutner, Linear cellular automata and DeBruijn automata, in: M. Delorme, J. Mazoyer (Eds.), Cellular Automata: A Parallel Model, Kluwer, Dordrecht, 1999.
[10] K. Sutner, Linear cellular automata and Fischer automata, Parallel Comput. 23 (11) (1997) 1613–1634.
[11] J. Von Neumann, in: A.W. Burks (Ed.), Theory of Self-reproducing Automata, University of Illinois Press, Urbana, IL, 1966.
[12] S. Wolfram, Statistical mechanics of cellular automata, Rev. Modern Phys. 55 (3) (1983) 601–644.